Sécurité sur l'Hébergement Web

Plusieurs couches de protection sont actives sur votre hébergement web.

Limites des ressources

Nos hébergements Standard fournissent une protection contre différentes attaques et qui se traduisent entres autres par une limitation des ressources disponibles pour un utilisateur donné. Ces limites sont définies selon le Forfait d'hébergement web souscrit.

Un outil permet de visualiser les limites qui ont été atteintes et ainsi mieux détecter les problèmes de performances ou de sécurité. Pour y accéder via DirectAdmin, aller dans le menu *Extra Features* → *Ressource Usage*. Par exemple :

https://srv1.kajoom.net:2222/CMD_PLUGINS/resource_usage/

Les paramètres évalués sont :

- CPU Usage : Limite les processeurs utilisés.
- Physical Memory Usage : Limite la mémoire-vive disponible.
- Input/Output Usage : Limite le débit d'upload et de download.
- IO operations : Limite le nombre d'opérations d'écriture et de lecture.
- Entry Processes (EP) : Limite les connexions concurrentes.
- Processes : Limite le nombre total de processus.

Lorsqu'une de ces limites est atteinte, elle apparaîtra en tant que faute (dans le tableau *Faults*).

Si cela devient fréquent, c'est soit un signe que :

- le site est visité par beaucoup de robots (bienveillants ou malveillants)
- le site est visité par beaucoup de vrais visiteurs

Dans le premier cas, tout est beau et la protection fait son travail!

Alors que dans le deuxième cas, cela voudrait dire que le compte nécessite une mise à niveau de forfait d'hébergement.

Pour en savoir plus :

- CloudLinux OS - Limits

Listes de blocages

Parmi les premières mesures de sécurité de base appliquées sur votre hébergement web, il y a les listes de blocages par adresse IP. Nous prenons en compte différentes sources afin de constituer une

protection globale et efficace contre les nouvelles menaces :

- Listes de “blacklists” publiques et réputées
- Firewall local actif et personnalisé sur chaque serveur

Que faire si mon adresse IP est présente dans une liste publique de blocages ?

Si votre adresse IP (de votre poste de travail ou de votre site web) se retrouve dans une block list publique, vous avez un problème!

- Contactez un expert ou un technicien informatique

Firewall Web Applicatif (WAF)

La protection pare-feu de type “Web Application Firewall” (WAF) permet de contrer de nombreuses attaques informatiques visant vos applications web PHP comme WordPress, Joomla ou Drupal pour ne nommer que ceux-là.

Notre équipe a mis au point un ensemble de règles personnalisées afin de vous permettre d'héberger vos sites dans un environnement sécuritaire.

Que faire si j'obtiens une erreur Not Acceptable - Error 406 ?

Dans certains cas, un blocage de type “Not Acceptable - Error 406” peut survenir lorsqu'une opération est faite sur votre site (demande d'une page, envoi d'un formulaire, sauvegarde de vos modifications).

Il est avisé de noter de noter :

- l'URL de la page sur laquelle vous étiez
- l'action que vous étiez en train de faire

L'interface de DirectAdmin permet dorénavant de modifier soi-même les paramètres de ModSecurity.

Pour ce faire, vous pouvez passer par les options disponibles sur la page de gestion des Domaines, par exemple :

https://srv1.kajoom.net:2222/user/domains

Ou bien aller directement dans les paramètres de ModSecurity, par exemple :

https://srv1.kajoom.net:2222/user/modsecurity

Protections anti-spam

De nombreuses mesures de protections contre le SPAM sont en place dans notre infrastructure. En voici un résumé.

- SpamAssassin
- Filtres par mots-clés
- Blocages par listes publiques
- Multiples vérifications contre le SPAM
- Scan antivirus
- Protections contre l'envoi abusif

En plus des dispositifs cités ci-dessous et si vos exigences en matière de SPAM sont très élevées, nous offrons un excellent service nommé Anti-Spam PRO qui répond à tous les besoins en termes de filtrage des courriels autant pour l'envoi que pour la réception.

Sauvegardes et réplication

Chaque serveur et chaque compte d'hébergement web fait l'objet de multiples sauvegardes et de réplication afin de parer au pire des événements. Parfois, ce n'est pas une catastrophe, mais c'est simplement pratique d'avoir accès à une sauvegarde antérieure de l'application web, de la base de données ou des fichiers.

Services reliés

- kajoom.ca/services/hebergement
- kajoom.ca/services/support-informatique
